UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In re Morgan Stanley Data Security Litigation	20 Civ. 5914 (AT)

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs John Nelson, Midori Nelson, and Sylvia Tillman ("California Plaintiffs"), Mark Blythe and Vivian Yates ("Florida Plaintiffs"), Cheryl Gamen and Richard Gamen ("Illinois Plaintiffs"), Amresh Jaijee, Richard Mausner, and Desiree Shapouri ("New York Plaintiffs"), and Howard Katz ("Pennsylvania Plaintiff") (collectively, "Plaintiffs") bring this Consolidated Class Action Complaint against Morgan Stanley Smith Barney, LLC ("Morgan Stanley" or "Defendant"), as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Morgan Stanley for its failure to properly secure and safeguard personal identifiable information, including without limitation, names, Social Security numbers, passport numbers, addresses, telephone numbers, email addresses, account numbers, dates of birth, income, asset value and holding information (collectively, "personal identifiable information" or "PII"). Plaintiffs also allege Morgan Stanley failed to provide timely, accurate, and adequate notice to Plaintiffs and similarly situated Morgan Stanley customers and former customers ("Class Members") that their PII had been lost, and precisely what types of information was unencrypted and in the possession of unknown third parties.

2. Not only did Morgan Stanley fail to secure and protect Plaintiffs' PII, but Morgan Stanley also retained Plaintiffs' PII far beyond the period required by any industry regulations—in some cases decades after those plaintiffs and class members closed their accounts and terminated their respective relationships with Morgan Stanley. Instead of observing appropriate destruction and clearinghouse practices, Morgan Stanley retained that PII for its continued economic and financial benefit.

3. Morgan Stanley sells securities and other financial products from offices nationwide. When individuals open a Morgan Stanley account, they are required to give the firm extensive PII for themselves and others associated with their accounts. Morgan Stanley retains this information in electronic form—for several years after a customer closes an account—and promises the public it will protect "the confidentiality and security of client information" by, among other things, using "computer safeguards and secured files and buildings."

4. This case does not involve a breach of a computer system by a third party, but rather an unauthorized disclosure of Plaintiffs' and Class Members' PII by Morgan Stanley to unknown third parties.

5. On or about July 9, 2020, Morgan Stanley began notifying various state Attorneys General of multiple data breaches that occurred as early as 2016. Around the same time, Morgan Stanley mailed a "Notice of Data Breach" to current and former customers affected by the breaches.

6. First, in 2016, Morgan Stanley closed two data centers and decommissioned its computer equipment. Morgan Stanley hired a vendor to remove customers' data from the equipment. Subsequently, Morgan Stanley learned that the equipment was not fully "wiped" clean, and that "certain devices believed to have been wiped of all information still contained some

unencrypted data." According to Morgan Stanley, that equipment went missing and currently Morgan Stanley does not know where this equipment is or who might have possession of it.

7. Second, in 2019, Morgan Stanley disconnected and replaced multiple computer servers in various branch locations. Those servers, which still contained customers' data, were thought to be encrypted, but Morgan Stanley subsequently learned that a "software flaw" on the servers left "previously deleted data" on the hard drives "in an unencrypted form." Now those servers are also missing (the 2016 and 2019 incidents will be collectively referred to herein as the "Data Breach").

8. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and the Class Members' PII, Morgan Stanley assumed legal and equitable duties to those individuals. Morgan Stanley admits that the unencrypted PII that has "left [its] possession" included PII from the account holders and any "individual(s) associated with your account(s), including account names and numbers (at Morgan Stanley and any linked bank accounts), Social Security number, passport number, contact information, date of birth, asset value and holdings data."

9. The missing equipment and servers contain all of the information unauthorized third-parties need to illegally use Morgan Stanley's current and former customers' PII to steal their identities and to make fraudulent purchases, among other things.

10. Not only can unauthorized third-parties access Morgan Stanley's customers' PII, that PII can be sold on the "dark web," a "black market" area of the internet not indexed by traditional search engines, where users anonymously engage in illicit activity, including rampant illegal commerce—including the sale of unencrypted, unredacted PII to criminals. Plaintiffs and Morgan Stanley's other current and former customers face a lifetime risk of identity theft, which

is heightened here by the exposure of their Social Security numbers and other PII used for illicit gain.

11. This PII was compromised due to Morgan Stanley's negligent and/or careless acts and omissions, and its failure to protect its customers' data. Morgan Stanley also failed to detect the Data Breach for years after it happened, and when it did discover the Data Breach, it took over a year, and possibly longer, to report it to the affected individuals and government authorities.

12. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. That risk will remain for their respective lifetimes.

13. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Morgan Stanley's failure to: (i) adequately protect its customers' PII; (ii) warn customers of its inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities. Morgan Stanley's conduct constitutes negligence and violates several state statutes as alleged herein.

14. Plaintiffs and Class Members have suffered injury as a result of Morgan Stanley's conduct. These injuries include: (i) the lost or diminished value of their PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under the California Unfair Competition Law (Cal. Business & Professions Code § 17200, *et seq*.) and similar consumer protection statutes in other states; and (v)

the continued and increased risk to their PII, which: (a) remains unencrypted and available on the missing equipment for unauthorized third parties to access and abuse; and (b) may remain backed up in Morgan Stanley's possession and is subject to further unauthorized disclosures so long as Morgan Stanley fails to undertake appropriate and adequate measures to protect the PII.

15. Morgan Stanley disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that its customers' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, Plaintiffs' and Class Members' PII was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and are entitled to injunctive and other equitable relief.

II. PARTIES

Plaintiffs

16. Plaintiffs John and Midori Nelson are citizens of California, residing in Antioch, California. Mrs. Nelson was the primary account holder of a Morgan Stanley IRA account. Mr. Nelson was the beneficiary of the IRA account. The account was closed on July 14, 2003. On or about July 15, 2020, the Nelsons received Morgan Stanley's Notice of Data Breach, dated July 10, 2020.

17. Plaintiff Sylvia Tillman is a citizen of California residing in San Diego County, California. In the early or mid-1990s, Ms. Tillman signed up for a California Uniform Transfers to Minors Act ("UTMA/CA") account for her minor daughter through Morgan Stanley in

California. A UTMA/CA account allows an appointed custodian to manage the minor's account until the latter turns 18. Ms. Tillman closed the UTMA/CA account in or about 2000, and has not been a Morgan Stanley client since that time. Ms. Tillman received Morgan Stanley's Notice of Data Breach, dated July 11, 2020, on or about that date. The notice specifically stated that the information associated with her UTMA/CA account was exposed by the Data Breach.

18. Plaintiff Mark Blythe is a Citizen of Florida residing in Flagler Beach, Florida. In or about 2012, Mr. Blythe signed up for a stock account and an annuity account through Morgan Stanley. On October 3, 2017 Mr. Blythe closed both of his accounts. Mr. Blythe received Morgan Stanley's Notice of Data Breach, dated July 11, 2020, on or about that date.

19. Plaintiff Vivian Yates is a citizen of Florida residing in Riverview, Florida. Ms. Yates signed up for a 529 college savings plan account at a Morgan Stanley office located in Florida, in or about 2015. The account is still open. Ms. Yates received Morgan Stanley's Notice of Data Breach, dated July 10, 2020, on or about that date.

20. Plaintiffs Richard Gamen and Cheryl Gamen, a married couple, are citizens of Illinois and reside in New Lenox, Illinois. In or about 1989, Richard and Cheryl Gamen signed up for a brokerage account through Morgan Stanley's office in Chicago, Illinois. In addition, Ms. Gamen rolled over her 401K individual retirement account to Morgan Stanley. Both the Gamens' accounts were closed in 2010 and 2001, respectively. Mr. and Mrs. Gamen each received Morgan Stanley's Notice of Data Breach, both dated July 11, 2020, on or about that date.

21. Plaintiff Amresh Jaijee is a citizen of New York residing in New York City. Ms. Jaijee signed up for a 401K individual retirement account at a Morgan Stanley office in New York in or about 2012. The account is still active. Ms. Jaijee received Morgan Stanley's Notice of Data Breach, dated July 10, 2020, on or about that date.

22. Plaintiff Richard Mausner is a citizen of New Jersey residing in Holmdel, New Jersey. Mr. Mausner had an account with Defendant in New Jersey, and closed it no later than 2010. He received Morgan Stanley's Notice of Data Breach dated July 11, 2020, on or about that date.

23. Plaintiff Desiree Shapouri is a Citizen of New York and resides in North Hills, New York. Ms. Shapouri had a Morgan Stanley account which she opened in New York in or about 2007. She closed the account in or about 2011. She received Morgan Stanley's Notice of Data Breach, dated July 11, 2020, on or about that date.

24. Plaintiff Howard Katz is a citizen of the Commonwealth of Pennsylvania, residing in Philadelphia. Mr. Katz signed up for his Morgan Stanley trading account in or about the end of 2012. Mr. Katz closed the account in or about 2016. On or about the week of July 20, 2020, Mr. Katz received Morgan Stanley's Notice of Data Breach, dated July 10, 2020.

Defendant

25. Defendant Morgan Stanley Smith Barney, LLC is a limited liability company organized under the laws of Delaware, headquartered at 1585 Broadway, New York, New York, with its principal place of business in New York, New York. Morgan Stanley Domestic Holdings, Inc. ("MSDHI"), a corporation organized under the laws of Delaware with its principal place of business in New York, New York, is the sole member of defendant Morgan Stanley Smith Barney, LLC. Defendant Morgan Stanley Smith Barney, LLC and its sole member, MSDHI, are both citizens of New York.

26. The true names and capacities of additional persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to

reflect the true names and capacities of such other responsible parties when their identities become known.

27. All of Plaintiffs' claims stated herein are asserted against Morgan Stanley and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

28. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member (including, for example, Plaintiff Sylvia Tillman, a citizen of California; Plaintiff Vivian Yates, a citizen of Florida; Plaintiffs Richard Gamen and Cheryl Gamen, citizens of Illinois) is a citizen of a state different from Defendant.

29. The Southern District of New York has personal jurisdiction over Defendant named in this action because Defendant is headquartered in this District and conducts substantial business in New York and this District through its headquarters, offices, and affiliates.

30. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered in this District and has caused harm to Plaintiffs and Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

Background

31. Morgan Stanley is a multinational investment bank and financial services company with offices in over 40 countries and more than 60,000 employees. The firm's clients include corporations, governments, institutions, and individuals. Morgan Stanley ranked 62nd in the 2019 Fortune 500 list of the largest United States corporations by total revenue.

32. Plaintiffs and Class Members, as current and former customers, relied on Morgan Stanley to keep their PII confidential and securely maintained, to use this information for its business purposes only, and to make only authorized disclosures of this information. Customers expect security to safeguard their PII, particularly from companies of Morgan Stanley's size and sophistication.

33. Morgan Stanley had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties. Morgan Stanley touts the security of its systems in its "Privacy Pledge":

> Morgan Stanley's long-standing commitment to safeguard the privacy of information our clients entrust to us is essential to our goal to be the world's first choice for financial services. **Protecting the confidentiality and security of client information has always been an integral part of how we conduct our business** worldwide.
>
> We pledge to continue to ensure that our global business practices protect your privacy. (emphasis added)[1]

34. Morgan Stanley also claims that the firm "use[s] personal information . . . to detect security incidents and protect against malicious, deceptive, fraudulent, or illegal activity."[2] The company further claims:

> To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. We have policies governing the proper handling of customer information by personnel and requiring third parties that

[1] Morgan Stanley's *Privacy Pledge*, *available at*: https://www.morganstanley.com/privacy-pledge (last visited November 1, 2020).

[2] Morgan Stanley's *U.S. Privacy Policy and Notice*, *available at*: https://www.morganstanley.com/disclaimers/us-privacy-policy-and-notice.html (last visited November 1, 2020).

> provide support to adhere to appropriate security standards with respect to such information.[3]

35. Morgan Stanley collects and maintains PII from its individual account holders, including but not limited to: "Social Security number and income;" "investment experience and risk tolerance;" and "checking account number and wire transfer instructions."[4]

36. Individual Morgan Stanley account holders may also supply the firm with personal identification (including passport numbers), mailing and billing addresses, telephone numbers, emails addresses, dates of birth, bank account numbers, and specific asset value and holdings information.

The Data Breach

37. Beginning on or about July 9, 2020, Morgan Stanley sent customers a "Notice of Data Breach."[5] Morgan Stanley, identifying itself as "Morgan Stanley Smith Barney LLC. Member SIPC / Morgan Stanley Private Bank, National Association. Member FDIC," informed the recipients of the notice that:

> In 2016, Morgan Stanley closed two data centers and decommissioned the computer equipment that processed client information in both locations. As is customary, we contracted with a vendor to remove the data from the devices. We subsequently learned that certain devices believed to have been wiped of all information still contained some unencrypted data. We have worked with outside technical experts to understand the facts and any potential risks [(the "Data Center Event")].[6]

---

[3] Morgan Stanley's *U.S. Customer Privacy Notice*, *available at*: https://www.morganstanley.com/disclaimers/im-customer-privacy-notice.pdf (last visited November 1, 2020).

[4] *Id.*

[5] *See Notice of Data Breach*, filed July 10, 2020 with the California Attorney General, a true and correct copy of which was previously filed at ECF No. 1-1.

[6] ECF No. 11, at 1.

38. On or about July 10, 2020, Morgan Stanley sent data breach notifications to various state Attorneys General, including Iowa's Attorney General Tom Miller, signed by Gerard Brady, Morgan Stanley's Chief Information Security Officer. Brady reported the 2016 incident above and added information about another related breach that began in 2019:

> Separately, in 2019, Morgan Stanley disconnected and replaced certain computer servers (the "WAAS device") in local branch offices. Those servers had stored information on encrypted disks that may have included personal information. During a recent inventory, we were unable to locate a small number of those devices. The manufacturer subsequently informed us of a software flaw that could have resulted in small amounts of previously deleted data remaining on the disks in unencrypted form. We have worked with outside technical experts to understand the facts and any potential risks (the "WAAS Device Event").[7]

39. Morgan Stanley admitted in the Notice of Data Breach and the letters to the Attorneys General that the hardware involved in both the 2016 Data Center Event and the 2019 WAAS Device Event "left our possession" at some point containing unencrypted information, and "it is possible that data associated with your account(s) could have remained on some of the devices when they left our possession."[8]

40. Morgan Stanley further admitted that the unencrypted PII that left its "possession" included information from the account holder and any "individual(s) associated with your account(s), including account names and numbers (at Morgan Stanley and any linked bank accounts), Social Security number, passport number, contact information, date of birth, asset value and holdings data."[9]

---

[7] *See Letter from Morgan Stanley's Gerard Brady to Iowa's Attorney General Tom Miller*, dated July 10, 2020, a true and correct copy of which was filed as ECF No. 1-2.

[8] ECF No. 1-2.

[9] ECF Nos. 1-1, 1-2.

41. For an UTMA/CA account, for example, the lost PII would include PII belonging to the UTMA/CA custodian managing the account and the minor account holder.

42. In response to the Data Breach, Morgan Stanley claims it has "instituted enhanced security procedures on your account(s), including continuous fraud monitoring and monitoring of information about malicious online activity and evidence of misuse of any Morgan Stanley data." It has also "taken steps to further strengthen controls aimed at reducing the risk that such an incident could occur in the future." [10]

43. The equipment containing Plaintiffs' and Class Members' unencrypted information is missing, and is or may become available for sale on the dark web, or fall into the hands of companies that will use the detailed PII for targeted marketing without the affected customers' approval. Unauthorized individuals can easily access Morgan Stanley's customers' unencrypted, unredacted information from these multiple devices, including Social Security numbers, passport numbers, addresses, telephone numbers, email addresses, checking account numbers, dates of birth, income, asset value and holding information.

44. Morgan Stanley did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for current and former customers, causing Plaintiffs' and Class Members' PII to be exposed.

Securing PII and Preventing Breaches

45. Morgan Stanley could have prevented this Data Breach by properly encrypting the lost equipment and computer files containing PII on those lost hard drives and, as Morgan Stanley claims it does, properly securing the "building" or location housing the equipment. Or Morgan Stanley could have destroyed the data, especially decades old data from former customers like

[10] ECF Nos. 1-1, 1-2.

Plaintiffs Cheryl Gamen, Richard Gamen, Richard Mausner, John Nelson, Midori Nelson, Desiree Shapouri, and Sylvia Tillman.

46. Morgan Stanley's negligence in safeguarding its customers' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing electronics. And Morgan Stanley, specifically, has suffered breaches that involved stolen equipment containing customer PII only two years before this Data Breach.[11] Morgan Stanley has acknowledged the sensitive and confidential nature of the PII. To be sure, collection, maintaining, and protecting PII is vital to many of Morgan Stanley's business purposes. Morgan Stanley has acknowledged through conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, Morgan Stanley failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being compromised.

47. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[12] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's

[11] Aruna Viswanatha, *Morgan Stanley Fined $1 Million for Client Data Breach*, The Wall Street Journal, June 8, 2016, *available at*: https://www.wsj.com/articles/morgan-stanley-fined-1-million-for-client-data-breach-1465415374 (last visited Oct. 16, 2020).

[12] 17 C.F.R. § 248.201 (2013).

license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[13]

48. The ramifications of Morgan Stanley's failure to keep its customers PII secure are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

49. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay for it on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[14] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[15]

50. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using

[13] *Id*.

[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 24, 2020).

[15] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed November 1, 2020).

> your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[16]

51. What is more, it is difficult to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraudulent activity to obtain a new number.

52. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center: "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

53. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—such as Social Security numbers, passport numbers, names, dates of birth, addresses, and asset holdings and other financial information.

54. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information,

---

[16] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 23, 2020).

[17] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited July 23, 2020).

personally identifiable information and Social Security numbers are worth more than 10x on the black market."[18]

55. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

56. The fraudulent activity resulting from the Data Breach may not come to light for years.

57. There may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[19]

58. At all relevant times, Morgan Stanley knew, or reasonably should have known, of the importance of safeguarding its current and former customers' PII, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Morgan Stanley's data security system was breached, including, specifically, the significant costs that would be imposed on Morgan Stanley's customers as a result of a breach.

---

[18] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 23, 2020).

[19] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last visited November 1, 2020).

59. Plaintiffs and Class Members now face years of diligent surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

60. Morgan Stanley was, or should have been, fully aware of the unique type and the significant volume of data on Morgan Stanley's decommissioned equipment, amounting to potentially millions of individuals' detailed, personal, finance-related information and thus, the significant number of individuals who would be harmed by the loss of decommissioned equipment containing unencrypted data.

61. To date, Morgan Stanley has offered its customers only two years of credit monitoring service through a single credit bureau, Experian. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

62. The injuries to Plaintiffs and Class Members were directly and proximately caused by Morgan Stanley's failure to implement or maintain adequate data security measures for its current and former customers' PII.

Morgan Stanley Failed to Comply with FTC Guidelines

63. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[20]

[20] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

64. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[21] The guidelines note businesses should protect the personal customer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

65. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[22]

66. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer and consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

67. Morgan Stanley was at all times fully aware of its obligation to protect the personal and financial data of consumers, including Plaintiffs and Class Members. Morgan Stanley was also aware of the significant repercussions if it failed to do so.

68. Morgan Stanley's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiffs' and members of the Classes Social Security numbers, dates of birth, and other highly sensitive and confidential

[21]Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

[22] FTC, *Start With Security*, *supra* note 5.

information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Morgan Stanley's Conduct Resulting in the Data Breach was Found to have been an Engagement in Unsafe or Unsound Practices Relating to Information Security and Noncompliance with 12 C.F.R. Part 30

69. On October 8, 2020, the Office of the Comptroller of the Currency ("OCC") entered into a Consent Order with Morgan Stanley (the "Consent Order"). A true and correct copy of the Consent Order is attached hereto as **Exhibit 1**.

70. Pursuant to the Consent Order, the OCC found that in 2016, Morgan Stanley failed to exercise proper oversight of the decommissioning of two Wealth Management business data centers located in the U.S., which is what led to the Data Breach and this litigation. Consent Order, § II(1).

71. The OCC further found that "[i]n connection with the decommissioning, [Morgan Stanley], among other things, failed to effectively assess or address the risks associated with the decommissioning of its hardware; failed to adequately assess the risk of using third party vendors, including subcontractors; and failed to maintain an appropriate inventory of customer data stored on the devices." Consent Order, § II(1).

72. The OCC further found that Morgan Stanley "failed to exercise adequate due diligence in selecting the third party vendor engaged by Morgan Stanley and failed to adequately monitor the vendor's performance." Consent Order, § II(1).

73. However, this violative behavior did not cease in 2016, and "[i]n 2019, [Morgan Stanley] experienced similar vendor management control deficiencies in connection with the decommissioning of wide area application services devices." Consent Order, § II(2).

74. Of great concern, only at the direction of the OCC did Morgan Stanley begin to notify "potentially impacted customers of the 2016 incident." Consent Order, § II(3).

75. Based on the foregoing and the full findings of the OCC in the Consent Order, it was determined that Morgan Stanley "was in noncompliance with 12 C.F.R. Part 30, Appendix B, 'Interagency Guidelines Establishing Information Security Standards,' and engaged in unsafe or unsound practices that were part of a pattern of misconduct." Consent Order, § II(5).

76. The Consent Order resulted in a fine of $60,000,000.00, Consent Order, § III(1), and a waiver of any rights to judicial review of the Consent Order. Consent Order, § IV(1).

Morgan Stanley's Customer Data was Previously Exposed in a Data Breach

77. In early 2015, several media outlets reported that Morgan Stanley had discovered data related to about 900 of its client accounts on Pastebin, during a review of websites known to post such information.[23] Morgan Stanley determined that those accounts were among nearly 350,000 accounts that Galen Marsh, a Morgan Stanley financial adviser, had downloaded from Morgan Stanley databases. *Id.* The Wall Street Journal subsequently described the incident as "what some security experts are saying is likely the biggest data theft at a wealth-management firm."[24] The Wall Street Journal later reported that in fact data related to about 1,200 Morgan

[23] Bloomberg News, *Financial Advisor Accused of Pilfering Data Working with Wirehouse*, Investment News (2015), *available at:* https://www.investmentnews.com/morgan-stanley-data-offered-on-internet-for-virtual-currency-60386 (last visited October 27, 2020).

[24] Justin Baer, *Puzzle Forms in Morgan Stanley Data Breach*, The Wall Street Journal, Jan. 7, 2015, *available at:* https://www.wsj.com/articles/puzzle-forms-in-morgan-stanley-data-breach-1420590326 (last visited October 22, 2020).

Stanley client accounts had appeared on Pastebin, and that the account information had "reappeared on several occasions" on other websites, including Twitter.[25]

78. In the course of a criminal proceeding against Mr. Marsh, the Department of Justice ("DOJ") disclosed that the Morgan Stanley software Mr. Marsh used to access the large volume of client data he downloaded was in fact supposed to limit his access to data related to his own clients. The Government's Sentencing Mem., at 2, *U.S. v. Marsh*, No. 15-cr-641 (D.D.C.), Dkt. No. 10 (filed Dec. 8, 2015). He was nevertheless able to conduct thousands of searches of other Morgan Stanley clients' data over a period of more than three years, during which he uploaded what was in fact data from over 700,000 clients to his own personal server. *Id.* at 3. Morgan Stanley's investigation revealed that hackers gained access to Mr. Marsh's personal server over a period of several weeks in October 2014. *Id.*

79. The Securities and Exchange Commission ("SEC") subsequently instituted an investigation that resulted in the disclosure of additional information. According to the SEC, "[b]etween approximately December 15, 2014 and February 3, 2015, portions of this stolen data were posted to at least three Internet sites along with an offer to sell a larger quantity of stolen data in exchange for payment in speedcoins, a digital currency." Order, at 2, *In re Morgan Stanley Smith Barney, LLC,* Admin. Proc. File No. 3-17280 (June 8, 2016).

80. Most significantly, the SEC found that Morgan Stanley: (1) "failed to ensure the reasonable design and proper operation of its policies and procedures in safeguarding confidential customer data"; (2) "failed to conduct any auditing or testing of the [deficient software modules]

[25] Justin Baer, *U.S. Shifts Focus of Morgan Stanley Breach Probe*, The Wall Street Journal, Feb. 18, 2015, *available at:* https://www.wsj.com/articles/u-s-shifts-focus-of-morgan-stanley-breach-probe-1424305501 (last visited October 22, 2020).

since their creation at least 10 years ago; and (3) "did not monitor user activity in the [deficient software modules] to identify any unusual or suspicious patterns. *Id.* at 3-4.

81. The SEC determined that Morgan Stanley had "willfully violated Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)), which requires every broker-dealer and investment adviser registered with the Commission to adopt written policies and procedures that are reasonably designed to safeguard customer records and information." *Id.* at 6 (footnote omitted). Morgan Stanley was censured and required to a pay a penalty of $1,000,000. *Id.*

Morgan Stanley's Collection and Use of PII

82. Morgan Stanley does not use its clients' personal and financial data only for the benefit of its clients. On information and belief, Defendant mines its collected data to apply data science applications to generate additional profit, or to sell that data to others to do the same. That is the most plausible explanation for Morgan Stanley's retention of its clients' data for decades after it was required to maintain that data.

83. Morgan Stanley's primary line of business encompasses financial advisory services.[26] To assist its wealth and asset management advisors in making "more informed decisions," Morgan Stanley uses machine-learning, a type of artificial intelligence ("AI") that allows computers to "'learn' by recognizing patterns and making inferences based on enormous

[26] *Artificial Intelligence at Morgan Stanley – Current Initiatives*, Business Intelligence and Analytics, April 7, 2020, *available at*: https://emerj.com/ai-sector-overviews/ai-morgan-stanley/ (last accessed Oct. 16, 2020).

sets of data."[27] Machine-learning engineers and data scientists are employed throughout Morgan Stanley, including Morgan Stanley's AI Center of Excellence ("CoE").[28]

84. CoE, employing at least 30 people, operates in New York and works with all of Morgan Stanley's operations, "from the financial advisors who work with Wealth Management clients to the traders who deal in complex securities."[29] CoE collects the required "enormous sets of data" from all departments, "helping these departments process the unstructured data they are collecting."[30] The collected data includes "text data stored internally, likely client emails, call logs, market research, and other digital assets."[31] The engineers collect everything, including "unstructured data from the internet, including articles and research on financial news websites."[32]

85. The relevant regulation requires Morgan Stanley to maintain client information for only five years after any activity related to an account. *See* 17 C.F.R. § 275.204–2(e)(1). Instead of destroying personal and sensitive financial data at that point, Morgan Stanley amassed enormous volumes of data without properly encrypting and physically securing it, in the pursuit of additional profits.

Morgan Stanley's Data Breach Caused Harm and will Result in Further Harm

86. The ramifications of Morgan Stanley's failure to keep Plaintiffs' and Class members' data secure are substantial.

---

[27] *Finding Professional Satisfaction in A.I. and Machine Learning*, Morganstanlet.com, *available at*: https://www.morganstanley.com/ideas/artificial-intelligence-center-of-excellence (last accessed Oct. 16, 2020).

[28] *Id*.

[29] *Id*.

[30] *Artificial Intelligence at Morgan Stanley*, *supra* note 26.

[31] *Id*.

[32] *Id*.

87. Consumer victims of data breaches are much more likely to become victims of identity fraud. This conclusion is based on an analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.[33]

88. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[34] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[35]

89. PII is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[36]

90. Identity thieves can use personal information, such as that of Plaintiffs and members of the classes, which Morgan Stanley failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

---

[33] 2014 LexisNexis True Cost of Fraud Study, https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

[34] 17 C.F.R § 248.201 (2013).

[35] *Id.*

[36] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited November 1, 2020).

91. Javelin Strategy and Research reports that identity thieves stole $112 billion from 2010 to 2016—which has increased since with the proliferation of data breaches.[37]

92. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[38]

93. An independent financial services industry research study conducted for BillGuard—a private enterprise that automates the consumer task of finding unauthorized transactions that might otherwise go undetected—calculated the average per-consumer cost of all unauthorized transactions at roughly $215 per cardholder incurring these charges,[39] some portion of which could go undetected and thus must be paid entirely out-of-pocket by consumer victims of account or identity misuse. This figure is based on misuse of cardholder information, which is less valuable than the PII at issue here—including full names, dates of birth, Social Security numbers, and other information which can easily be used to open credit accounts and other financial accounts to perpetrate further fraud, increasing the amount of average damages.

---

[37] *https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point*

[38] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf.

[39] Hadley Malcom, *Consumers rack up $14.3 billion in gray charges, research study commissioned for Billguard by Aite Research, USA Today* (July 25, 2013), available at: https://www.usatoday.com/story/money/personalfinance/2013/07/25/consumers-unwanted-charges-in-billions/2568645/.

94. Thus, Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

California Plaintiff John and Midori Nelson's Experience

95. On November 11, 2000, Ms. Nelson opened her IRA account at Morgan Stanley with the assistance of her brother, who was then employed at Morgan Stanley as a financial analyst. When opening her account, Ms. Nelson listed her husband, John Nelson, as the sole beneficiary of all proceeds of her IRA account. Morgan Stanley asked Ms. Nelson to supply her and Mr. Nelson's PII, including but not limited to their names, address and Social Security numbers. Ms. Nelson closed her account on July 14, 2003 after her brother stopped working for Morgan Stanley.

96. Mr. and Mrs. Nelson received the *Notice of Data Breach*, dated July 10, 2020, on or about that date. It was addressed to "John C. Nelson & Midori T. Nelson JT Ten."

97. In or about June 2019, unknown third parties used Ms. Nelson's credit card to make unauthorized purchases. Her credit card company confirmed the fraud and reimbursed her. Later in 2019, unknown third parties used the same credit card account to make unauthorized purchases. The credit card company again confirmed the fraud and reimbursed the account. Both times, the Nelsons were unable to use the credit card for approximately one week before each card was replaced by mail.

98. As a result of the Data Breach notice and the fraudulent credit card charges, Mr. and Mrs. Nelson have spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach*, reviewing their financial accounts statements, visiting their bank and contacting their credit union and credit card companies about possible financial consequences, and routinely monitoring their credit for suspicious activity on credit bureau websites. Moreover, over the past few years, the Nelsons have repeatedly received

phishing telephone calls. The calls became so frequent they purchased an electronic device designed to block these messages. This time and expense can never be recovered, and particularly for Ms. Nelson, who suffers from chronic and often debilitating illness, it is time spent suffering through tasks that needlessly tax her physically, mentally and emotionally.

99. Mr. and Mrs. Nelson are very careful about sharing their PII, and have never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

100. Mr. and Mrs. Nelson suffered actual injury and damages in paying annual fees to Defendant for facilitating Ms. Nelson's trading account before the Data Breach, expenditures that they would not have incurred had Defendant disclosed that it lacked data security practices adequate to safeguard customers' PII.

101. Mr. and Mrs. Nelson suffered actual injury in the form of damages to and diminution in the value of his PII -- a form of intangible property – that they both entrusted to Morgan Stanley for the purpose of facilitating Ms. Nelson's retirement account, which was compromised in the Data Breach.

102. Mr. and Mrs. Nelson suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and have anxiety and increased concerns for the loss of their privacy.

103. Mr. and Mrs. Nelson have suffered and will continue to suffer imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII, especially their Social Security numbers, being placed in the hands of criminals and other unauthorized third parties.

104. Mr. and Mrs. Nelson have a continuing interest in ensuring that their PII that remains backed up in Morgan Stanley's computer systems and is sufficiently protected and safeguarded from future data breaches.

California Plaintiff Sylvia Tillman's Experience

105. In the early or mid-1990s, Plaintiff Sylvia Tillman signed up for a California Uniform Transfers to Minors Act ("UTMA/CA") account for her minor daughter through Morgan Stanley in California. A UTMA/CA account allows an appointed custodian to manage the minor's account until the latter turns 18. Ms. Tillman supplied Morgan Stanley with her and her daughters' PII, including but not limited to her address and Social Security number. Ms. Tillman closed the UTMA/CA account in or about 2000. At the time of the Data Breach, Ms. Tillman was not a Morgan Stanley client.

106. Ms. Tillman supplied Morgan Stanley with her and her daughters' PII, including but not limited to her address and Social Security number. Ms. Tillman closed the UTMA/CA account in or about 2000. At the time of the Data Breach, Ms. Tillman was not a Morgan Stanley client.

107. Ms. Tillman received the Notice of Data Breach, dated July 11, 2020, on or about that date. It was addressed to "Sylvia Tillman cust[odian] for [her minor daughter] UTMA/CA."

108. As a result of the Data Breach notice, Ms. Tillman spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, communicating with Morgan Stanley representatives on the toll-free number supplied in the notice, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost and cannot be recaptured.

109. Ms. Tillman is very careful about sharing her PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

110. Ms. Tillman stores any and all documents containing her PII in a safe and secure digital location, and destroys any documents she receives in the mail that contain any of her PII, or that may contain any information that could otherwise be used to compromise her credit card accounts and identity. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

111. Ms. Tillman suffered actual injury and damages in paying money to Morgan Stanley for facilitating the UTMA/CA account before the Data Breach; expenditures which she would not have made had Morgan Stanley disclosed that it lacked data security practices adequate to safeguard customers' PII.

112. Ms. Tillman suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Ms. Tillman entrusted to Morgan Stanley for the purpose of facilitating the UTMA/CA account, which was compromised in and as a result of the Data Breach.

113. Ms. Tillman suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

114. Ms. Tillman has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her and her daughters' Social Security numbers, being placed in the hands of unauthorized third-parties and possibly criminals.

115. Ms. Tillman has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Morgan Stanley's possession, is protected and safeguarded from future breaches.

Florida Plaintiff Mark Blythe's Experiences

116. In or about 2012, Plaintiff Mark Blythe signed up for a stock account and an annuity account through Morgan Stanley. Mr. Blythe supplied Morgan Stanley with PII, including but not limited to his name address, and Social Security number. Both accounts were closed on October 3, 2017.

117. Mr. Blythe received the *Notice of Data Breach*, dated July 10, 2020, on or about July 28, 2020.

118. In or about July 2020, Mr. Blythe suffered a string of identity thefts involving the Navy Federal Credit Union in Virginia and misuse of his personal information through no fault of his own. On or about July 6, 2020, an unauthorized third party opened a checking account with a credit union in Mr. Blythe's name. On or about July 7, 2020, an unauthorized third party applied for a Small Business Administration ("SBA") loan with the same credit union in Mr. Blythe's name. On or about July 15, 2020, an unauthorized third party opened a savings account in Mr. Blythe's name. On or about July 17, 2020, Mr. Blythe learned of the identity theft because of the credit union directly reporting to Experian, with whom Mr. Blythe had purchased credit monitoring. Specifically, the credit union pulled Mr. Blythe's credit during the process of making an SBA loan to an unauthorized third party.

119. As a result of the Data Breach notice and identity theft, Mr. Blythe spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach*, communicating with credit reporting agencies, and by

investigating and attempting to stop fraudulent uses of his compromised PII by unauthorized third parties, which included filing a police report with the Flagler Beach Police Department and notifying a credit union multiple times of fraudulent uses of Mr. Blythe's PII at that credit union. Additionally, Mr. Blythe now monitors his credit regularly using Experian professional software and when these issues arose, he immediately contacted Experian, the credit union and other authorities. Having learned of the identify theft, Mr. Blythe and his wife both went into credit lock due to the fraudulent activity. Post-breach, Mr. Blythe maintained his "Professional Credit Monitoring Profile" with Experian. This time has been lost forever and cannot be recaptured.

120. Mr. Blythe is very careful about sharing his PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Prior to the recent fraudulent transactions, Mr. Blythe has not experienced fraud or identity theft.

121. Mr. Blythe stores any and all documents containing his PII in a safe and secure digital location, and destroys any documents he receives in the mail that contain any of her PII, or that may contain any information that could otherwise be used to compromise his credit card accounts and identity. Moreover, he diligently chooses unique usernames and passwords for her various online accounts.

122. Mr. Blythe suffered actual injury and damages in paying money to Morgan Stanley for facilitating his stock account and an annuity account; expenditures which he would not have made had Morgan Stanley disclosed that it lacked data security practices adequate to safeguard customers' PII.

123. Mr. Blythe suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Mr. Blythe entrusted to Morgan Stanley for the purpose of facilitating his stock account and annuity account, which was compromised in and

as a result of the Data Breach.

124. Mr. Blythe suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

125. Mr. Blythe has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

126. Mr. Blythe has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Morgan Stanley's possession, is protected and safeguarded from future breaches.

Florida Plaintiff Vivian Yates' Experiences

127. Vivian Yates signed up for her 529 college savings plan account at a Morgan Stanley office located in Florida, in or about 2015. Ms. Yates supplied Morgan Stanley with her PII, including but not limited to her name, address, Social Security number, and other financial information.

128. Ms. Yates received Morgan Stanley's Notice of Data Breach, dated July 10, 2020, on or about that date.

129. As a result of the Data Breach notice, Ms. Yates spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, communicating with Morgan Stanley representatives on the toll-free number supplied in the notice, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

130. Ms. Yates is very careful about sharing her PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

131. Ms. Yates stores any and all documents containing her PII in a safe and secure digital location, and destroys any documents she receives in the mail that contain any of her PII, or that may contain any information that could otherwise be used to compromise her credit card accounts and identities. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

132. Ms. Yates suffered actual injury and damages in paying money to Morgan Stanley for facilitating her accounts before the Data Breach; expenditures which she would not have made had Morgan Stanley disclosed that it lacked data security practices adequate to safeguard customers' PII.

133. Ms. Yates suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Morgan Stanley for the purpose of facilitating her accounts, which was compromised in and as a result of the Data Breach.

134. Ms. Yates suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

135. Ms. Yates has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her lost PII, especially her Social Security number being placed in the hands of unauthorized third parties and possibly criminals.

136. Ms. Yates has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Morgan Stanley's possession, is protected and safeguarded from future breaches.

Illinois Plaintiffs Richard and Cheryl Gamen's Experiences

137. In or about 1989, Plaintiffs Richard Gamen and his wife, Cheryl Gamen, signed up for a brokerage account through Morgan Stanley's office in Chicago, Illinois. Mr. and Mrs. Gamen supplied Morgan Stanley with their PII, including but not limited to their names, address and Social Security numbers. The brokerage account was terminated in or about 2010.

138. Mrs. Gamen, in the early 1990's, also rolled over her 401K individual retirement account to Morgan Stanley. That account was terminated in or about 2001.

139. Mr. and Mrs. Gamen received a joint Notice of Data Breach, dated July 11, 2020, on or about that date, for the brokerage account. Ms. Gamen received another Notice of Data Breach, dated July 11, 2020, on or about July 26, 2020, for her IRA account.

140. In or about June 2020, Mr. Gamen began receiving an increasing number of scam telephone calls on a regular basis. The calls claim his Social Security number is "locked" and that he will be arrested unless he interacts with the caller. Mr. Gamen has also received an increasing number of emails from fraudsters claiming a foreign person has died and the fraudster is reaching out to share the money.

141. As a result of the Data Breach notices and the scam calls and emails, Mr. Gamen spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, communicating with Morgan Stanley representatives on the toll-free number supplied in the notice, exploring credit monitoring and identity theft insurance options, and self-monitoring their accounts. Mr. Gamen also filed an online complaint with the Federal Trade Commission regarding this Data Breach. This time has been lost forever and cannot be recaptured.

142. Mr. and Ms. Gamen are very careful about sharing their PII, and have never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

143. Mr. Gamen stores any and all documents containing their PII in a safe and secure digital location, and destroys any documents they receive in the mail that contain any of their PII, or that may contain any information that could otherwise be used to compromise their credit card accounts and identities. Moreover, they diligently choose unique usernames and passwords for their various online accounts.

144. Mr. and Mrs. Gamen suffered actual injury and damages in paying money to Morgan Stanley for facilitating their accounts before the Data Breach; expenditures which they would not have made had Morgan Stanley disclosed that it lacked data security practices adequate to safeguard customers' PII.

145. Mr. and Mrs. Gamen suffered actual injury in the form of damages to and diminution in the value of their PII—a form of intangible property that Mr. and Mrs. Gamen entrusted to Morgan Stanley for the purpose of facilitating their accounts, which was compromised in and as a result of the Data Breach.

146. Mr. and Mrs. Gamen suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and have anxiety and increased concerns for the loss of their privacy.

147. Mr. and Mrs. Gamen have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their lost PII, especially their Social Security numbers being placed in the hands of unauthorized third parties and possibly criminals.

148. Mr. and Mrs. Gamen have a continuing interest in ensuring that their PII, which, upon information and belief, remains backed up in Morgan Stanley's possession, is protected and safeguarded from future breaches.

New York Plaintiff Amresh Jaijee's Experience

149. In or about 2012, Plaintiff Amresh Jaijee rolled over her 401K individual retirement account ("IRA") to Morgan Stanley at one of Morgan Stanley's offices in New York City. Ms. Jaijee supplied Morgan Stanley with her PII, including but not limited to her name, address, Social Security number, personal identification, checking account number and other financial information. She listed beneficiaries to her account and included their contact information. Ms. Jaijee's Morgan Stanley account is still active.

150. Ms. Jaijee received the Notice of Data Breach, dated July 10, 2020, on or about that date. It specifically states that in addition to her Social Security number, information about "any linked bank accounts" was breached as well.

151. In or around the end of June 2020, Ms. Jaijee received a telephone call from an individual claiming to represent an insurance company. This individual knew her Social Security number and attempted to have her verify it and her bank routing number. Ms. Jaijee later called the insurance company and confirmed her suspicions that the earlier call was a scam.

152. Since in or about June 2020, Ms. Jaijee has received an increasing number of scam telephone calls, some displaying "JP Morgan/Chase" on her Caller ID, but the corresponding messages are in Chinese.

153. As a result of the Data Breach notice and the scam telephone calls, Ms. Jaijee spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and the insurance company call, communicating with

representatives of her bank that is linked to the Morgan Stanley IRA, alerting her credit card companies and the three credit bureaus about the breach, routinely checking her credit monitoring (for which she continues to pay approximately $18 per month), exploring further credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

154. Ms. Jaijee attempted to use the Experian credit monitoring offered by Morgan Stanley, but was not successful. She contacted Experian to assist her in signing up, but the technician told her that "passwords were being updated" and that someone from Experian would contact her to assist. To date, Ms. Jaijee is waiting to hear back from Experian. She is still unable to register with Experian despite having the Notice of Data Breach addressed to her.

155. Ms. Jaijee stores any and all documents containing her PII in a safe and secure digital location, and destroys any documents she receives in the mail that contain her Social Security number or any other vital PII. Moreover, she diligently chooses unique usernames and passwords for her various online accounts, and routinely changes those passwords.

156. Ms. Jaijee suffered actual injury and damages in paying annual fees to Morgan Stanley for facilitating her 401K IRA account before the Data Breach; expenditures which she would not have made had Morgan Stanley disclosed that it lacked data security practices adequate to safeguard customers' PII.

157. Ms. Jaijee suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Ms. Jaijee entrusted to Morgan Stanley for the purpose of facilitating her 401K IRA account, which was compromised in and as a result of the Data Breach.

158. Ms. Jaijee suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy, especially her Social Security number. Ms. Jaijee was recently contacted by an unidentified party by telephone that had her Social Security number and asked her to verify it. With the new information that her Social Security number has been lost by Morgan Stanley, this concerns her even more.

159. Ms. Jaijee has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number being placed in the hands of unauthorized third-parties and possibly criminals.

160. Ms. Jaijee has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Morgan Stanley's possession, is protected and safeguarded from future breaches.

New York Plaintiff Richard Mausner's Experience

161. Plaintiff Richard Mausner signed up for an account at Morgan Stanley in New Jersey. Mr. Mausner supplied Morgan Stanley with his PII, including but not limited to his name, address and Social Security number in connection with the opening of this account. Mr. Mausner closed the account no later than 2010.

162. Mr. Mausner received the Notice of Data Breach, dated July 11, 2020, on or about that date.

163. As a result of the Data Breach notice, Mr. Mausner spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, placing a credit freeze, contacting his bank, exploring credit monitoring and identity theft insurance options, and self- monitoring his accounts. This time has been lost forever

and cannot be recaptured.

164. Mr. Mausner stores documents containing his PII in a safe and secure digital location, and destroys any documents he receives in the mail that contain any of his PII, or that may contain any information that could otherwise be used to compromise his credit card accounts and identity. Moreover, he diligently chooses unique usernames and passwords for his online accounts.

165. Mr. Mausner suffered actual injury and damages in paying money to Morgan Stanley for facilitating his account before the Data Breach; expenditures which he would not have made had Defendant disclosed that it lacked data security practices adequate to safeguard customers' PII.

166. Mr. Mausner suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Mr. Mausner entrusted to Defendant for the purpose of facilitating his account, which was compromised in and as a result of the Data Breach.

167. Mr. Mausner suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

168. Mr. Mausner has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his lost PII, especially his Social Security number being placed in the hands of unauthorized third parties and possibly criminals.

169. Mr. Mausner has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

New York Plaintiff Desiree Shapouri's Experience

170. Plaintiff Desiree Shapouri signed up for an account at Morgan Stanley in New York in or about 2007.Ms. Shapouri was asked to and did supply Morgan Stanley with her PII, including but not limited to her address and Social Security number in connection with the opening of this account. Ms. Shapouri closed her account in or about 2011.

171. Ms. Shapouri received the Notice of Data Breach, dated July 11, 2020, on or about that date.

172. From September 3, 2019 through September 18, 2019 Ms. Shapouri experienced twelve separate unauthorized charges on her American Express credit card.

173. As a result of the Data Breach notice, Ms. Shapouri spent time dealing with the consequences of the Data Breach, which includes exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. She also initiated a credit frees with TransUnion and Equifax, as well as purchased identify theft protection with Identify Guard. This time has been lost forever and cannot be recaptured.

174. Ms. Shapouri is very careful about sharing her PII, and stores documents containing her PII in a safe and secure digital location, and destroys documents she receives in the mail that may contain her PII, or that may contain any information that could otherwise be used to compromise her credit card accounts and identity. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

175. Ms. Shapouri suffered actual injury and damages in paying money to Morgan Stanley for facilitating his stock account and an annuity account; expenditures which he would not have made had Morgan Stanley disclosed that it lacked data security practices adequate to safeguard customers' PII.

176. Ms. Shapouri suffered actual injury in the form of damages to and diminution in

the value of her PII—a form of intangible property that Ms. Shapouri entrusted to Defendant for the purpose of facilitating her account, which was compromised in and as a result of the Data Breach.

177. Ms. Shapouri suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

178. Ms. Shapouri has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, her Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

179. Ms. Shapouri has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Pennsylvania Plaintiff Howard Katz' Experience

180. In or about the end of 2012, Plaintiff Howard Katz signed up for a trading account at Morgan Stanley via telephone. When he opened his account, Morgan Stanley asked Mr. Katz to supply his PII, including but not limited to his name, address, and Social Security number. Mor. Katz closed the account in or about 2016.

181. Mr. Katz received the Notice of Data Breach, dated July 10, 2020, on or about that date, addressed to "Howard Katz."

182. As a result of the Data Breach notice and the related fraudulent charges and contacts, Mr. Katz spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, checking his credit monitoring (which he continues to pay approximately $125 per year), exploring further credit monitoring and identity theft insurance options, visiting his bank to report the debit card fraud, and self-monitoring

his accounts. This time has been lost forever and cannot be recaptured.

183. Mr. Katz is very careful about sharing his PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

184. Mr. Katz stores any and all information containing his PII in a safe and secure digital location, and destroys any documents he receives in the mail that contain any of his PII, or that may contain any information that could otherwise be used to compromise his credit card accounts and identity. Moreover, Mr. Katz diligently chooses unique usernames and passwords for his various online accounts.

185. Mr. Katz suffered actual injury and damages in paying annual fees to Defendant for facilitating his trading account before the Data Breach, expenditures that he would not have incurred had Defendant disclosed that it lacked data security practices adequate to safeguard customers' PII.

186. Mr. Katz suffered actual injury in the form of damages to and diminution in the value of his PII – a form of intangible property – that Mr. Katz entrusted to Morgan Stanley for the purpose of facilitating his trading account, which was compromised in the Data Breach.

187. Mr. Katz suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

188. Mr. Katz has suffered and will continue to suffer imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of criminals and other unauthorized third parties.

189. Mr. Katz has a continuing interest in ensuring that his PII that remains backed up in Morgan Stanley's computer systems and is sufficiently protected and safeguarded from future data breaches.

V. CLASS ALLEGATIONS

190. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

191. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals residing in the United States whose PII was compromised in the data breach first announced by Morgan Stanley on or about July 9, 2020 (the "Nationwide Class").

192. The Nationwide Class that Plaintiffs Cheryl Gamen, Richard Gamen, Richard Mausner, John Nelson, Midori Nelson, Desiree Shapouri, and Sylvia Tillman additionally seek to represent is defined as follows:

> All individuals residing in the United States who had closed their accounts with Morgan Stanley at least five years prior to the Data Breach and whose PII was compromised in the data breach first announced by Morgan Stanley on or about July 9, 2020 (the "Former Customer Nationwide Class").

193. The California Subclass, who Plaintiffs John Nelson, Midori Nelson, and Sylvia Tillman (the "California Plaintiffs") seek to represent is defined as follows:

> All individuals residing in California whose PII was compromised in the data breach first announced by Morgan Stanley on or about July 9, 2020 (the "California Subclass").

194. Plaintiffs John Nelson, Midori Nelson, and Sylvia Tillman additionally seek to represent the following subclass defined as follows:

> All individuals residing in California who had closed their accounts with Morgan Stanley at least five years prior to the Data Breach and

> whose PII was compromised in the data breach first announced by Morgan Stanley on or about July 9, 2020 (the "Former Customer California Subclass").

195. The Florida Subclass, who Plaintiffs Mark Blythe and Vivian Yates (the "Florida Plaintiffs") seek to represent is defined as follows:

> All individuals residing in Florida whose PII was compromised in the data breach first announced by Morgan Stanley on or about July 9, 2020 (the "Florida Subclass").

196. The Illinois Subclass, who Plaintiffs Cheryl and Richard Gamen (the "Illinois Plaintiffs") seek to represent is defined as follows:

> All individuals residing in Illinois whose PII was compromised in the data breach first announced by Morgan Stanley on or about July 9, 2020 (the "Illinois Subclass").

197. Plaintiffs Cheryl and Richard Gamen additionally seek to represent the following subclass defined as follows:

> All individuals residing in Illinois who had closed their accounts with Morgan Stanley at least five years prior to the Data Breach and whose PII was compromised in the data breach first announced by Morgan Stanley on or about July 9, 2020 (the "Former Customer Illinois Subclass").

198. The New York Subclass, who Plaintiffs Amresh Jaijee, Richard Mausner, and Desiree Shapouri (the "New York Plaintiffs") seek to represent is defined as follows:

> All individuals residing in New York whose PII was compromised in the data breach first announced by Morgan Stanley on or about July 9, 2020 (the "New York Subclass").

199. Plaintiffs Richard Mausner and Desiree Shapouri additionally seek to represent the following subclass defined as follows:

> All individuals residing in New York who had closed their accounts with Morgan Stanley at least five years prior to the Data Breach and whose PII was compromised in the data breach first announced by

> Morgan Stanley on or about July 9, 2020 (the "Former Customer New York Subclass").

200. The Pennsylvania Subclass, who Plaintiff Howard Katz seeks to represent is defined as follows:

> All persons residing in Pennsylvania whose PII was compromised in the data breach first announced by Morgan Stanley on or about July 9, 2020 (the "Pennsylvania Subclass").

201. The above classes and subclasses are herein referred to as the "Classes."

202. Excluded from the Classes are the following individuals and/or entities: Morgan Stanley and Morgan Stanley's parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Morgan Stanley has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

203. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

204. Numerosity, Fed R. Civ. P. 23(a)(1): Classes are so numerous that joinder of all members is impracticable. Morgan Stanley has identified thousands of customers whose PII may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Morgan Stanley's records.

205. Commonality and predominance, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Morgan Stanley had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Morgan Stanley had respective duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Morgan Stanley had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Morgan Stanley failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. Whether and when Morgan Stanley actually learned of the Data Breach;

f. Whether Morgan Stanley adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Morgan Stanley violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Morgan Stanley failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Morgan Stanley adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Morgan Stanley engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Morgan Stanley's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Morgan Stanley's wrongful conduct;

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach;

n. Whether Morgan Stanley violated the California Unfair Competition Law (Business & Professions Code § 17200, *et seq*.);

o. Whether Morgan Stanley violated the California Consumer Privacy Act (Cal. Civ. Code § 1798.100, *et seq.* (§ 1798.150(a));

p. Whether Morgan Stanley violated the Illinois Consumer Fraud Act, 815 Ill. Comp. Stat. 505/1, *et seq*.

q. Whether Morgan Stanley violated the New York Consumer Law for Deceptive Acts and Practices New York Gen. Bus. Law § 349;

r. Whether Morgan Stanley violated New York's Data Breach Notification Law, N.Y. Gen. Bus. Law § 899-aa; and

a. Whether Morgan Stanley violated Pennsylvania's Unfair Trade Practices and Consumer Protection Law, UTPCPL 73 § 202-1 & 202-3, *et seq*.

206. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Morgan Stanley's misfeasance.

207. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Morgan Stanley has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate

with respect to the Class as a whole. Morgan Stanley's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Morgan Stanley's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

208. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously.

209. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Morgan Stanley. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

210. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure

to afford relief to Plaintiffs and Class Members for the wrongs alleged because Morgan Stanley would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

211. The litigation of the claims brought herein is manageable. Morgan Stanley's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

212. Adequate notice can be given to Class Members directly using information maintained in Morgan Stanley's records.

213. Unless a Class-wide injunction is issued, Morgan Stanley may continue in its failure to properly secure the PII of Class Members, Morgan Stanley may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Morgan Stanley may continue to act unlawfully as set forth in this Complaint.

214. Further, Morgan Stanley has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

215. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Morgan Stanley owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Morgan Stanley breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Morgan Stanley failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Morgan Stanley on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Morgan Stanley breached the implied contract;

f. Whether Morgan Stanley adequately, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Morgan Stanley failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Morgan Stanley engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,

i. Whether Class Members are entitled to actual damages, statutory damages, injunctive relief, and/or punitive damages as a result of Morgan Stanley's wrongful conduct.

VI. APPLICATION OF NEW YORK LAW TO THE NATIONWIDE CLASSES

216. The laws of New York should govern Plaintiffs' claims and, therefore, the claims of the Nationwide Classes that Plaintiffs seek to represent.

217. Morgan Stanley is headquartered at 1585 Broadway, New York, New York, with its principal place of business in New York, New York. Upon information and belief, the headquarters is the "nerve center" of Morgan Stanley's business activities—the place where its executive-level and similarly-responsible officers, directors, and other high-level employees direct, control, and coordinate the corporation's activities, including its data security functions and major policy and legal decisions.

218. New York has a significant interest in regulating the conduct of businesses operating within its borders. New York, which seeks to protect the rights and interests of residents and citizens of the United States against financial companies headquartered and doing business in New York, has a greater interest in the nationwide claims of Plaintiffs and members of the Classes than any other state and is mot intimately concerned with the claims and outcome of this litigation.

219. Upon information and belief, all contracts that Plaintiffs and members of the classes reviewed and executed were created by Morgan Stanley in New York.

220. Upon information and belief, all monies that Plaintiffs and members of the classes made to Morgan Stanley for its products were ultimately delivered to Morgan Stanley in New York.

221. Upon information and belief, Morgan Stanley's clearinghouse practices and decisions related thereto—including the disposal of servers and computer equipment at issue in this Data Breach—were made from and in New York.

222. Upon information and belief, Morgan Stanley's response to the Data Breach, and the decisions and responses thereto, were made from and in New York.

223. Application of New York law to Plaintiffs' and members of the classes claims would be neither arbitrary nor fundamentally unfair because New York has a significant interest in the claims of Plaintiffs and members of the Classes.

224. Under choice of law principles applicable to this litigation, the common law of New York would apply to the nationwide common law claims, as well as the New York law claims, of all class members because New York's significant interest in regulating the conduct of businesses—Morgan Stanley included—operating within its borders. Thus, New York's consumer protection laws may be applied to non-resident consumers across the United States.

225. Alternatively, the law governing Plaintiffs' common law claims alleged herein on behalf of both Nationwide Classes of current and former Morgan Stanley customers does not differ materially across the states in which Class Members reside or create predominating individual issues of law sufficient to impede the certification of both Nationwide Classes.

COUNT I
Negligence
(On Behalf of Plaintiffs and both Nationwide Classes, or in the alternative, on behalf of the Subclasses)

226. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 225.

227. As a condition of their using the services of Morgan Stanley, customers were obligated to provide Morgan Stanley with certain PII, including their date of birth, mailing addresses, Social Security numbers, passport numbers and personal financial information.

228. Plaintiffs and Class Members entrusted their PII to Morgan Stanley on the premise and with the understanding that Morgan Stanley would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

229. Morgan Stanley has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

230. Morgan Stanley knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of their customers' PII involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

231. Morgan Stanley had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Morgan Stanley's security protocols to ensure that Plaintiffs' and Class Members' information in Morgan Stanley's possession was adequately secured and protected.

232. Morgan Stanley also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

233. Morgan Stanley also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and Class Members' PII.

234. Morgan Stanley's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and Class Members entrusted Morgan Stanley with their confidential PII, a necessary part of the process of establishing an account with the company.

235. Morgan Stanley was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or Class Members.

236. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class Members was reasonably foreseeable, particularly in light of Morgan Stanley's inadequate security practices and previous breach incidents involving Morgan Stanley customers' PII on stolen equipment.

237. Plaintiffs and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Morgan Stanley knew of should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Morgan Stanley's systems.

238. Morgan Stanley's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Morgan Stanley's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Morgan Stanley's misconduct also included its decisions not to comply with industry standards for the safekeeping

of Plaintiffs' and Class Members' PII, including basic encryption techniques freely available to Morgan Stanley.

239. Plaintiffs and the Class Members had no ability to protect their PII that was in, and possibly remains in, Morgan Stanley's possession.

240. Morgan Stanley was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

241. Morgan Stanley had and continues to have a duty to adequately disclose that the PII of Plaintiffs and Class Members within Morgan Stanley's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

242. Morgan Stanley had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and Class Members.

243. Morgan Stanley has admitted that the PII of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

244. Morgan Stanley, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and Class Members during the time the PII was within Morgan Stanley's possession or control.

245. Morgan Stanley improperly and inadequately safeguarded the PII of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

246. Morgan Stanley failed to heed industry warnings and alerts to provide adequate safeguards to protect customers' PII in the face of increased risk of theft.

247. Morgan Stanley, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its customers' PII.

248. Morgan Stanley breached its duty to exercise appropriate clearinghouse practices by failing to remove former customers' PII it was no longer required to retain pursuant to regulations.

249. Morgan Stanley, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

250. But for Morgan Stanley's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII of Plaintiffs and Class Members would not have been compromised.

251. There is a close causal connection between Morgan Stanley's failure to implement security measures to protect the PII of Plaintiffs and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiffs and the Class. Plaintiffs' and Class Members' PII was lost and accessed as the proximate result of Morgan Stanley's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

252. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Morgan Stanley, of failing to use reasonable measures to protect PII. The FTC

publications and orders described above also form part of the basis of Morgan Stanley's duty in this regard.

253. Morgan Stanley violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Morgan Stanley's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

254. Morgan Stanley's violation of Section 5 of the FTC Act constitutes negligence *per se*.

255. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

256. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

257. As a direct and proximate result of Morgan Stanley's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover

from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Morgan Stanley's possession and is subject to further unauthorized disclosures so long as Morgan Stanley fails to undertake appropriate and adequate measures to protect the PII of customers in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Morgan Stanley's goods and services they received.

258. As a direct and proximate result of Morgan Stanley's negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

259. Additionally, as a direct and proximate result of Morgan Stanley's negligence and negligence *per se*, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Morgan Stanley's possession and is subject to further unauthorized disclosures so long as Morgan Stanley fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT II
Invasion of Privacy
(On Behalf of Plaintiffs and both Nationwide Classes, or in the alternative, on behalf of the Subclasses)

260. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 225.

261. Plaintiffs and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

262. Morgan Stanley owed a duty to its customers, including Plaintiffs and Class Members, to keep their PII contained as a part thereof, confidential.

263. Morgan Stanley failed to protect and released to unknown and unauthorized third parties the PII of Plaintiffs and Class Members.

264. Morgan Stanley allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiffs and Class Members, by way of Morgan Stanley's failure to protect the PII.

265. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and Class Members is highly offensive to a reasonable person.

266. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII to Morgan Stanley as part of its use of Morgan Stanley's services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

267. The Data Breach at the hands of Morgan Stanley constitutes an intentional interference with Plaintiffs and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

268. Morgan Stanley acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

269. Because Morgan Stanley acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class Members.

270. As a proximate result of the above acts and omissions of Morgan Stanley, the PII of Plaintiffs and Class Members was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

271. Unless and until enjoined, and restrained by order of this Court, Morgan Stanley's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Morgan Stanley can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiffs and both Nationwide Classes, or in the alternative, on behalf of the Subclasses)

272. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 225.

273. Plaintiffs plead this claim in the alternative to their common law and statutory claims alleged herein.

274. Plaintiffs and Class Members conferred a monetary benefit on Morgan Stanley. Specifically, they purchased goods and services from Morgan Stanley and provided Morgan

Stanley with their PII. In exchange, Plaintiffs and Class Members should have received from Morgan Stanley the goods and services that were the subject of the transaction and should have been entitled to have Morgan Stanley protect their PII with adequate data security.

275. Morgan Stanley appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members and it accepted and retained that benefit. Morgan Stanley profited from the purchases and used the PII of Plaintiffs and Class Members for business purposes.

276. Plaintiffs' and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

277. The amounts Plaintiffs and Class Members paid for Morgan Stanley's goods and services should have been used, in part, to pay for the administrative costs of data management and security, including the proper and safe disposal of Plaintiffs' and Class Members' PII.

278. Under the principles of equity and good conscience, Morgan Stanley should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Morgan Stanley failed to implement the data management and security measures that are mandated by industry standards.

279. Morgan Stanley failed to secure the PII of Plaintiffs and Class Members and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

280. Morgan Stanley acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

281. If Plaintiffs and Class Members knew that Morgan Stanley would not secure their PII using adequate security, they would not have made purchases or developed a financial relationship with Morgan Stanley.

282. Plaintiffs and Class Members have no adequate remedy at law.

283. As a direct and proximate result of Morgan Stanley's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Morgan Stanley's possession and is subject to further unauthorized disclosures so long as Morgan Stanley fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Morgan Stanley's goods and services they received.

284. As a direct and proximate result of Morgan Stanley's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

285. Morgan Stanley should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from Plaintiffs and Class Members. In the alternative, Morgan Stanley should be

compelled to refund the amounts that Plaintiffs and Class Members overpaid for Morgan Stanley's goods and services.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiffs and both Nationwide Classes, or in the alternative, on behalf of the Subclasses)

286. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 225.

287. At all times during Plaintiffs' and Class Members' interactions with Morgan Stanley, Morgan Stanley was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' PII that Plaintiffs and Class Members provided to Morgan Stanley.

288. As alleged herein and above, Morgan Stanley's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

289. Plaintiffs and Class Members provided their respective PII to Morgan Stanley with the explicit and implicit understandings that Morgan Stanley would protect and not permit the PII to be disseminated to any unauthorized third parties.

290. Plaintiffs and Class Members also provided their respective PII to Defendant with the explicit and implicit understandings that Morgan Stanley would take precautions to protect that PII from unauthorized disclosure.

291. Morgan Stanley voluntarily received in confidence Plaintiffs' and Class Members' PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

292. Due to Morgan Stanley's failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

293. As a direct and proximate cause of Morgan Stanley's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

294. But for Morgan Stanley's disclosure of Plaintiffs' and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Morgan Stanley's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as the resulting damages.

295. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Morgan Stanley's unauthorized disclosure of Plaintiffs' and Class Members' PII. Morgan Stanley knew or should have known its methods of accepting and securing Plaintiffs' and Class Members' PII was inadequate as it relates to, at the very least, disposal of servers and other equipment containing Plaintiffs' and Class Members' PII.

296. As a direct and proximate result of Morgan Stanleys' breach of its confidence with Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of

the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Morgan Stanley's goods and services they received.

297. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT V
Violations of New York Consumer Law for Deceptive Acts and Practices New York Gen. Bus. Law § 349
(On Behalf of Plaintiffs and both Nationwide Classes, or in the alternative, on behalf of New York Plaintiffs and the New York Subclasses)

298. All Plaintiffs (or alternatively The New York Plaintiffs) ("Plaintiffs," for purposes of this Count), individually and on behalf of the Nationwide Class (or alternatively, on behalf of the other New York Subclass members), re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 192, 198, 199, and 202 through 225.

299. New York General Business Law ("NYGBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

300. By reason of the conduct alleged herein, Morgan Stanley has engaged in unlawful practices within the meaning of the NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of the NYGBL § 349, and the deception occurred within New York State.

301. Morgan Stanley stored Plaintiffs' and the Class members' PI on the aforementioned servers. Morgan Stanley knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiffs' and the Class members' PI secure and prevented the loss or misuse of Plaintiffs' and the Class members' PII. Defendant did not disclose to Plaintiffs and the Class members that the disposal of the servers was not in a secure manner.

302. Plaintiffs and the Class never would have provided their sensitive and personal PII if they had been told or knew that Morgan Stanley would fail to maintain sufficient security to keep such PII from being taken by others.

303. Morgan Stanley violated the NYGBL §349 by misrepresenting, both by affirmative conduct and by omission, the safety of Morgan Stanley's storage and services, specifically the security thereof, and their ability to safely store and dispose of Plaintiffs' and the Class members' PII.

304. Morgan Stanley also violated NYGBL §349 by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to immediately notify Plaintiffs and the Class members of the Data Breach. If Morgan Stanley had complied with these legal requirements, Plaintiffs and the other Class members would not have suffered the damages related to the Data Breach.

305. Morgan Stanley's practices, acts, policies and course of conduct violate NYGBL § 349 in that:

a. Morgan Stanley actively and knowingly misrepresented or omitted disclosure of material information to Plaintiffs and the Class at the time they provided such PII that Morgan Stanley did not have sufficient security or mechanisms to protect PII;

b. Morgan Stanley failed to give timely warnings and notices regarding the defects and problems with the disposal of their serves to protect Plaintiffs' and the Class' PII. Morgan Stanley possessed prior knowledge of the inherent risks in its disposal practices.

306. Plaintiffs and the Class were entitled to assume, and did assume, Morgan Stanley would take appropriate measures to keep their PII safe. Morgan Stanley did not disclose at any time that Plaintiffs' and the Class' PI was vulnerable to malicious actors due to Morgan Stanley's disposal practices, and Morgan Stanley was the only one in possession of that material information, which it had a duty to disclose.

307. The aforementioned conduct is and was deceptive, false, and fraudulent and constitutes an unconscionable commercial practice in that Morgan Stanley has, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the inadequate nature of its disposal practices, resulting in the Data Breach.

308. Members of the public were deceived by and relied upon Morgan Stanley's misrepresentations and failures to disclose.

309. Such acts by Morgan Stanley are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her PII to Morgan Stanley.

Said deceptive acts and practices are material. The requests for and use of such PII in New York through deceptive means occurring in New York were consumer-oriented acts and thereby falls under the New York consumer fraud statute, NYGBL § 349.

310. Morgan Stanley's wrongful conduct caused Plaintiffs and the Classes to suffer a consumer-related injury by causing them to incur substantial expense to protect from misuse of the PII by third parties and placing the Plaintiffs and the Classes at serious risk for monetary damages.

311. As a direct and proximate result of Morgan Stanley's violations of the above, Plaintiffs and Class members suffered damages including, but not limited to:

a. unauthorized use of their PII;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PII;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection

services, initiating and monitoring credit freezes, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. damages to and diminution in value of their PII entrusted to Morgan Stanley, and the loss of Plaintiffs' and Class members' privacy.

312. In addition to or in lieu of actual damages, because of the injury, Plaintiffs and the Classes seek statutory damages for each injury and violation which has occurred

COUNT VI
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful Business Practices
(On Behalf of the California Plaintiffs and the California Subclasses)

313. California Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 17, 25 through 115, 193, 194, and 202 through 215.

314. Morgan Stanley has violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the California Class.

315. Morgan Stanley engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting California Plaintiffs' and California Subclass Members' PII with knowledge that the information would not be adequately protected; and by storing California Plaintiffs' and California Subclass Members' PII in an unsecure environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Morgan Stanley to take reasonable methods of safeguarding the PII of California Plaintiffs and the California Subclass Members.

316. In addition, Morgan Stanley engaged in unlawful acts and practices by failing to disclose the Data Breach to California Plaintiffs and the California Subclass Members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

317. As a direct and proximate result of Morgan Stanley's unlawful practices and acts, California Plaintiffs and the California Subclass Members were injured and lost money or property, including but not limited to the price received by Morgan Stanley for the services, the loss of California Plaintiffs' and California Subclass Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

318. Morgan Stanley knew or should have known that Morgan Stanley's computer systems and data security practices were inadequate to safeguard California Plaintiffs' and California Subclass Members' PII and that the risk of a data breach or theft was highly likely, especially given Morgan Stanley's inability to adhere to basic encryption standards and data disposal methodologies. Morgan Stanley's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the California Plaintiffs and California Subclass Members.

319. California Plaintiffs and California Subclass Members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to California Plaintiffs and California Subclass Members of money or property that Morgan Stanley may have acquired by means of Morgan Stanley's unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Morgan Stanley because of Morgan Stanley's unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT VII
Violation of California's Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*. – Unfair Business Practices
(On Behalf of the California Plaintiffs and the California Subclasses)

320. California Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 17, 25 through 115, 193, 194, and 202 through 215.

321. Morgan Stanley engaged in unfair acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting California Plaintiffs' and California Subclass Members' PII with knowledge that the information would not be adequately protected; by storing California Plaintiffs' and California Subclass Members' PII in an unsecure electronic environment; and by failing to properly dispose of equipment containing sensitive PII. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to California Plaintiffs and California Subclass Members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to California Plaintiffs and the California Subclass Members outweighed their utility, if any.

322. Morgan Stanley engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect California Plaintiffs' and California Subclass Members' PII from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to California Plaintiffs and California Subclass Members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to California Plaintiffs and the California Subclass Members outweighed their utility, if any.

323. As a direct and proximate result of Morgan Stanley's acts of unfair practices, California Plaintiffs and the California Subclass Members were injured and lost money or property, including but not limited to the price received by Morgan Stanley for the services, the loss of California Plaintiffs' and California Subclass Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

324. Morgan Stanley knew or should have known that Morgan Stanley's computer systems and data security practices were inadequate to safeguard California Plaintiffs' and California Subclass Members' PII and that the risk of a data breach or theft was highly likely, including Morgan Stanley's failure to properly encrypt and dispose of equipment containing sensitive PII. Morgan Stanley's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of California Plaintiffs and California Subclass Members.

325. California Plaintiffs and California Subclass Members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to California Plaintiffs and California Subclass Members of money or property that Morgan Stanley may have acquired by means of Morgan Stanley's unfair business practices, restitutionary disgorgement of all profits accruing to Morgan Stanley because of Morgan Stanley's unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT VIII
Violation of the California Consumer Privacy Act,
Cal. Civ. Code § 1798.100, *et seq.* (§ 1798.150(a))
(On Behalf of California Plaintiffs and the California Subclasses)

326. California Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 17, 25 through 115, 193, 194, and 202 through 215.

327. Morgan Stanley violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent California Plaintiffs' and California Subclass Members' PII from unauthorized access and exfiltration, theft, or disclosure as a result of Morgan Stanley's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of California Plaintiffs and California Class Members.

328. As a direct and proximate result of Morgan Stanley's acts, California Plaintiffs' and the California Subclass Members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure as a result of Morgan Stanley's violation of the duty.

329. As a direct and proximate result of Morgan Stanley's acts, California Plaintiffs and the California Subclass Members were injured and lost money or property, including but not limited to the price received by Morgan Stanley for the services, the loss of California Class Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

330. Morgan Stanley knew or should have known that its data security and clearinghouse practices were inadequate to safeguard California Plaintiffs' and California Subclass Members' PII and that the risk of a data breach or theft was highly likely. Morgan Stanley failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of California Plaintiffs and the California Class members.

331. Morgan Stanley is a limited liability company that is organized or operated for the profit or financial benefit of its owners, with annual gross revenues over $25 million. Morgan Stanley collects consumers' PII as defined in Cal. Civ. Code § 1798.140.

332. California Plaintiffs and California Subclass Members seek relief under § 1798.150(a), including, but not limited to, recovery of actual damages; statutory damages; injunctive or declaratory relief; any other relief the court deems proper; and attorneys' fees and costs.

COUNT IX
Violation of the Illinois Consumer Fraud Act
815 Ill. Comp. Stat. 505/1, *et seq.*
(On Behalf of Illinois Plaintiffs and on behalf of the Illinois Subclasses)

333. Illinois Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 15, 20, 25 through 94, 137 through 148, 196, 197, and 202 through 215.

334. Morgan Stanley, while operating in Illinois, used and employed unfair and deceptive acts and practices, including deception and misrepresentation, in the conduct of trade or commerce, and unfair acts and practices, fraud, misrepresentation, and the concealment, suppression, and omission of material facts with the intent that others rely on such concealment, suppression and omission, in connection with the sale and advertisement of services, in violation of 815 Ill. Comp. Stat. 505/2. This includes but is not limited to the following:

a. Morgan Stanley failed to enact adequate privacy and security measures to protect Illinois Plaintiffs' and the Illinois Subclass Members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Morgan Stanley failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Morgan Stanley knowingly and fraudulently misrepresented that they would maintain adequate data privacy and security practices and procedures to safeguard Illinois Plaintiff's and the Illinois Subclass Members' PII from unauthorized disclosure, release, data breaches, and theft;

d. Morgan Stanley failed to properly vet and determine that the disposal of the servers would meet industry standards and regulations;

e. Morgan Stanley knowingly omitted, suppressed, and concealed the inadequacy of its privacy and security protections for Illinois Plaintiffs' and the Illinois Subclass Members' PII;

f. Morgan Stanley knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Illinois Plaintiffs' and the Illinois Subclass Members' PII;

g. Morgan Stanley failed to maintain the privacy and security of Illinois Plaintiffs' and the Illinois Subclass Members' PII, in violation of duties imposed by applicable federal and state laws, which was a direct and proximate cause of the Data Breach; and

h. Morgan Stanley failed to disclose the Data Breach to Illinois Plaintiffs and the Illinois Subclass Members in a timely manner, in violation of the duties imposed by 815 Ill. Comp. Stat. § 530/10(a).

335. As a direct and proximate result of Morgan Stanley's practices, Illinois Plaintiffs and the Illinois Subclass Members suffered the injury and/or damages described herein, including but not limited to the following:

a. unauthorized use of their PII;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PII;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, initiating and monitoring credit freezes, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach.

336. The above unfair and deceptive practices and acts by Morgan Stanley were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Illinois Plaintiffs and the Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

337. Morgan Stanley knew or should have known that their computer systems, data security practices, and disposal practices were inadequate to safeguard Illinois Plaintiffs' and the Illinois Subclass Members' PII and that the risk of a data breach or theft was highly likely. Morgan Stanley's actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Illinois Plaintiffs and the Illinois Subclass Members.

338. Illinois Plaintiffs and the Illinois Subclass Members seek relief under 815 Ill. Comp. Stat. 505/10a, including but not limited to damages, restitution and punitive damages (to be proven at trial), injunctive relief, and/or attorneys' fees and costs.

COUNT X
Violation of New York's Data Breach Laws – Delayed Notification
(N.Y. Gen. Bus. Law § 899-aa)
(On Behalf of New York Plaintiffs and the New York Subclass)

339. New York Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 15, 21 through 23, 25 through 94, 149 through 179, 198, 199, and 202 through 215.

340. Section 899-aa(3) of NYGBL requires any "person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization."

341. Section 899(5) of NYGBL states:

> The notice required by this section shall be directly provided to the affected persons by one of the following methods:
>
> (a) written notice;
>
> (b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the

> person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction;
>
> (c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or
>
> (d) Substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. Substitute notice shall consist of all of the following:
>
> (1) e-mail notice when such business has an e-mail address for the subject persons;
>
> (2) conspicuous posting of the notice on such business's web site page, if such business maintains one; and
>
> (3) notification to major statewide media.

342. The Data Breach described in this Complaint constitutes a "breach of the security system" of Morgan Stanley.

343. As alleged above, Morgan Stanley unreasonably delayed informing New York Plaintiffs and the New York Subclass Members about the Data Breach, affecting the confidential and non-public PII of New York Plaintiffs and the New York Subclass Members after Morgan Stanley knew the Data Breach had occurred.

344. Morgan Stanley failed to disclose to New York Plaintiffs and the New York Subclass Members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PII when Morgan Stanley knew or reasonably believed such information had been compromised.

345. Morgan Stanley's ongoing business interests gave Morgan Stanley incentive to conceal the Data Breach from the public to ensure continued revenue.

346. As a result of Morgan Stanley's violation of New York law, New York Plaintiffs and the New York Subclass Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, including securing identity theft protection, or requesting a credit freeze. These measures would have prevented some or all of the damages New York Plaintiffs and the New York Subclass Members suffered because their stolen information would not have any value to identity thieves.

347. As a result of Morgan Stanley's violation of New York law, New York Plaintiffs and the New York Subclass Members have suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

348. New York Plaintiffs and the New York Subclass Members seek all remedies available under New York law, including, but not limited to damages the New York Plaintiffs and the New York Subclass Members suffered as alleged above, as well as equitable relief.

COUNT XI
Violation of Pennsylvania's Unfair Trade Practices and Consumer Protection Law, UTPCPL 73 § 201-2 & 202-3, *et seq.*
(On Behalf of Plaintiff Howard Katz and the Pennsylvania Subclass)

349. Plaintiffs Howard Katz ("Plaintiff," for purposes of this Count) re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 15, 24 through 94, 180 through 189, 200, and 202 through 215.

350. Morgan Stanley, Plaintiff, and the Pennsylvania Subclass Members are "Person[s]" within the meaning of Pennsylvania Unfair Trade Practices and Consumer Protection Law ("UTPCPL" 73 PS § 201, et seq.).

351. The Pennsylvania UTPCPL 73 PS § 201-3 declares unlawful "unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce …."

352. Morgan Stanley's business acts and practices alleged herein constituted deceptive acts or practices under Pennsylvania UTPCPL 73 PS § 201, *et seq.*

353. Morgan Stanley engaged in deceptive acts or practices by engaging in the course of conduct described herein.

354. Morgan Stanley knew or should have known of vulnerabilities and defects in the disposal of Plaintiff's and the Pennsylvania Subclass Members' PII before the Data Breach but concealed that information in violation of the UTPCPL.

355. Morgan Stanley engaged in deceptive acts and practices by failing to disclose and actively concealing known data-security disposal defects, and by otherwise deceiving Plaintiff and the Pennsylvania Subclass Members.

356. More specifically, Morgan Stanley engaged in deceptive trade practices by:

a. Misrepresenting or omitting material facts to Plaintiff and the Pennsylvania Subclass Members regarding the adequacy of Morgan Stanley's data security procedures protecting PII in violation of 73 Pa. Cons. Stat. §201-3(4) (v), (vii), (ix) and (xxi);

b. Misrepresenting or omitting material facts to Plaintiff and the Pennsylvania Subclass Members regarding Morgan Stanley's failure to comply with relevant state and federal laws designed to protect consumers' privacy and PII in violation of 73 Pa. Cons. Stat. §201-3(4)(v), (vii), (ix), and (xxi);

c. Failing to discover and disclose the Data Breach to Plaintiff and the Pennsylvania Subclass Members in a timely manner in violation of 73 Pa. Cons, Stat §2303(a); and

d. Engaging in unfair, unlawful, and deceptive acts and practices by failing to maintain the privacy and security of Plaintiff's and the Pennsylvania Subclass Members' PII, in violation of duties imposed by public policies reflected in applicable federal and state laws, resulting in the Data Breach. These deceptive acts and practices were likely to and did deceive Plaintiff and the Pennsylvania Subclass Members regarding the lack of security protecting their PII.

357. Morgan Stanley intentionally and knowingly misrepresented such material facts with an intent to mislead the Plaintiff and the Pennsylvania Subclass Members.

358. The above unlawful, unfair, and deceptive acts and practices by Morgan Stanley were immoral, unethical, oppressive and unscrupulous. These acts caused substantial injury to Plaintiff and the Pennsylvania Subclass Members that they could not reasonably avoid, this substantial injury outweighed any benefits to consumers or to competition.

359. Morgan Stanley owed to Plaintiff and the Pennsylvania Subclass Members a duty to disclose its data-security disposal defects because Morgan Stanley possessed exclusive knowledge regarding the vulnerability of the PII, concealed these defects from Plaintiff and the Pennsylvania Subclass Members, and made incomplete representations regarding its data security systems while withholding material facts from Plaintiff and the Pennsylvania Subclass Members.

360. These representations and omissions were material to Plaintiff and the Pennsylvania Subclass Members due to the value and sensitivity of the PII.

361. Plaintiff and the Pennsylvania Subclass Members suffered ascertainable loss as a result of Morgan Stanley's misrepresentations, concealment, and omissions of material information as alleged herein.

362. As a direct and proximate result of Morgan Stanley's violation of UTPCPL, Plaintiff and the Pennsylvania Subclass Members have suffered damages including, but not limited to:

a. unauthorized use of their PII;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PII;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, initiating and monitoring credit freezes, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach.

363. Plaintiff and the Pennsylvania Subclass Members seek an order enjoining Morgan Stanley's deceptive acts and practices, and awarding attorneys' fees, and any other just and proper relief available under UTPCPL.

364. In addition to or in lieu of actual damages, Plaintiff and the Pennsylvania Subclass Members seek statutory damages for each injury and violation which has occurred.

365. Plaintiff and the Pennsylvania Subclass Members seek relief under 73 Pa. Cons. Stat.§201-9.2, including, but not limited to, injunctive relief, actual damages, or $100 per Pennsylvania Subclass Member, whichever is greater, treble damages, and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against Morgan Stanley and that the Court grant the following:

A. For an Order certifying the Nationwide Classes or, in the alternative, the Subclasses as defined above, and appointing Plaintiffs and their Counsel to represent the certified Classes;

B. For equitable relief enjoining Morgan Stanley from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiffs and Class Members;

C. For equitable relief compelling Morgan Stanley to use appropriate cyber security methods and policies with respect to PII collection, storage, protection, and disposal, and to disclose with specificity to Plaintiffs and Class Members the type of PII compromised;

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: November 2, 2020

Respectfully Submitted,

MORGAN & MORGAN

By: /s/ Jean S. Martin
Jean S. Martin
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jmartin@ForThePeople.com

NUSSBAUM LAW GROUP, P.C.

By: /s/ Linda P. Nussbaum
Linda P. Nussbaum
1211 Avenue of the Americas, 40th Fl.
New York, NY 10036
(917) 438-9189
lnussbaum@nussbaumpc.com

Interim Co-Lead Counsel for Class Plaintiffs